De factoribus numerorum compositorum dignoscendis

Disquisitio Academica,

cujus partem secundam,

adnuente amplissima Fac. Philos.

Præside

CAROLO JOH. D^S HILL,

Math. Prof. Reg. & Ord.

pro summis in philosophia capessendis honoribus

exhibet

J. WESTERBERG,

Scanus.

In Academia Carolina Die IX Junii MDCCCXXXVIII.

LUNDÆ,

TYPIS EXCUDIT C. FR. BERLING,

UNIVERSITATIS TYPOGRAPHUS.

MDCCCXXXVIII.

5) Similiter progredi licet ad potentias altiores ipsius 2, et regulæ invenientur, quæ nihil nisi dimidiationem et additionem simplicem expostulant. Sit ex. gr.

$N \underset{64}{\backsim} 0$, et $N = a + a_1 10 + a_2 10^2 + a_3 10^3 + a_4 10^4 + a_5 10^5 + A 10^6$, eritque $N \underset{26}{\backsim} a + 10a_1 + 36a_2 + 40a_3 + 16a_4 + 32a_5 \underset{64}{\backsim} 0$. At jam invenimus $a + 10a_1 + 4a_2 = 8(\gamma + a_1)$, quia $N \underset{16}{\backsim} 0$, atque $\gamma + a_1 + a_3 = 2\delta$. Erit igitur

$N \underset{64}{\backsim} 8(\gamma + a_1) + 32a_2 + 8a_3 + 32a_3 + 16a_4 + 32a_5$, seu $N \underset{64}{\backsim} 8.2\delta + 32(a_2 + a_3 + a_5) + 16a_4 \underset{64}{\backsim} 0$. Quoniam vero et $N \underset{32}{\backsim} 0$, poni potest $\delta + a_4 = 2\varepsilon$; eritque ita $N \underset{64}{\backsim} 16.2\varepsilon + 32(a_2 + a_3 + a_5) \underset{64}{\backsim} 0$, ideoque $\varepsilon + a_2 + a_3 + a_5 \underset{2}{\backsim} 0$; unde regulam facile elicies.

Ex. gr. $N = \overset{a_5}{7}\ \overset{a_4}{0}\ \overset{a_3}{6}\ \overset{a_2}{1}\ \overset{a_1}{4} \mid \overset{a}{4} : 2\ (=\alpha)$	*) $\varepsilon = 3 = (0 + 6) : 2$
$\alpha = +2 \mid$	$a_2 = 1$
$\beta = +3 \mid 6 : 2\ (=\beta)$	$a_3 = 6$
$\gamma = +2 \mid 4 : 2\ (=\gamma)$	$a_5 = 7$
$\alpha_1 = +4 \mid$	$17 \underset{2}{\backsim} 1$, non vero
$\delta = +6 \mid 12 : 2\ (=\delta)$	$17 \underset{2}{\backsim} 0$; quare hic N per 2^6
$\varepsilon = 3 \mid 6 \mid : 2\ (=\varepsilon)$*)	haud dividitur; sed tantum
17	per 2^5.

Commodius tamen interdum numerus datus prævie per 32 aut per 1024, quoties licet, dividitur; aut etiam schemata primi generis adhibentur, qualia sunt, præter universale $\left(\begin{matrix} & +\nu \\ o & . \end{matrix}\right)$ ad 2^ν pertinens, hæc $\left(\begin{matrix} & +\nu \\ \alpha & \end{matrix}\right)$ ad divisorem 2^n pertinentia:

$\left(\begin{matrix} & -III \\ 24 & . \end{matrix}\right)$ ad 2^{10}, 2^9, 2^8, 2^7, (2^6) et $\left(\begin{matrix} & +III \\ 40 & . \end{matrix}\right)$ ad 2^6; $\left(\begin{matrix} & +V \\ 160 & . \end{matrix}\right)$ ad 2^9 et 2^8, $\left(\begin{matrix} & +IV \\ 16 & . \end{matrix}\right)$ ad 2^7; $\left(\begin{matrix} & +III \\ 8 & . \end{matrix}\right)$ ad 2^4, et $\left(\begin{matrix} & +II \\ 4 & . \end{matrix}\right)$ ad 2^4 et 2^3, nec non $\left(\begin{matrix} & +I \\ 2 & . \end{matrix}\right)$ ad 2^3. Sic in eodem Ex. $\left(\begin{matrix} & -III \\ 24 & . \end{matrix}\right) N =$

$= 144 - 24.706 = - 16800$, iterumque $\begin{pmatrix} -III \\ 24\ . \end{pmatrix}^2 N = - \begin{pmatrix} -III \\ 24\ . \end{pmatrix}$ $16800 = -800 + 24.16 = -416$; aut $\overset{+III}{40\ .}\ N = 40.706 + 144 = 28\,384$, iterumque $40.28 + 384 = 1504$ et denuo $40.1 + 504 = 544$. Sed 544 et -416 per 2^6 divisa æque residuum 32 relinquunt, quod (ideoque et N) per 2^5 dividitur. — Numeri vero hi auxiliares α et ν inveniuntur modo mox dicendo. Pergimus interim factores, ad schemata data pertinentes, perquirere.

II) Ponamus igitur alterius $\alpha = 1$, et $\beta = \pm 1$, ut habeamus schema $\begin{pmatrix} \pm & \nu \\ 1 & . & 1 \end{pmatrix}$ seu $\begin{pmatrix} \pm & \nu \\ 1 & . \end{pmatrix}$ seu $\begin{pmatrix} \nu & \pm \\ . & 1 \end{pmatrix}$, quod ad numerum $10^\nu \mp 1$ hujusve factores attinet, qui inveniuntur istum numerum (qui formæ est 999...99 aut 1000...001), in factores simplices (vel primos) resolvendo; quo facto, quoniam $\begin{pmatrix} +n \\ 1\ . \end{pmatrix}$ est schema factorum ipsius $10^n - 1$, et $\begin{pmatrix} -n \\ 1\ . \end{pmatrix}$ ipsius $10^n + 1$, erit

cum n	$\begin{pmatrix} +n \\ 1\ . \end{pmatrix}$ ad factores	et $\begin{pmatrix} -n \\ 1\ . \end{pmatrix}$ schema ad factores
= 1.	$3,\ 3^2 = 9$	11.
2.	$3^2.\ 11 = (99)$	101.
3.	$3^3.\ 37 = (999)$	$7.11.13 = (1001)$
4.	$(99).101$	$73.137 = (10001)$
5.	$3^2.\ 41.271.$	$11.9091.$
6.	$(999).(1001)$	101.9901
7.	$3^2.\ 239.4649.$	11.909091
8.	$(9999).(10001).$	$17.5\,882353$
9.	$3^4.\ 37.333667$	$(1001).19.52579.$

n	$\left(\begin{smallmatrix}+n\\ 1\ .\end{smallmatrix}\right)$	$\left(\begin{smallmatrix}-n\\ 1\ .\end{smallmatrix}\right)$
= 10.	3^2 (100001).(11111)	101.99 009901.
11.	3^2 [11111 111111]	11^2 23.[35 932447]
12.	(999999).(1000001)	(10001).99 990001.
13.	3^2 53.79.[265 371653].	11.[909090 909091]
14.	$(10^7-1).(10^7+1)$.	29.101.281.[121 499449]
15.	3^3 31.37.41.271.[2906161]	7.11.13.211.241.2161.9091.

Hos factores olim directe perquisivimus *). Postmodum vero schemata hujus $\left(\begin{smallmatrix}+n\\ 1\ .\end{smallmatrix}\right)$ vel generalioris $\left(\begin{smallmatrix}+n\\ \beta\ .\ \alpha\end{smallmatrix}\right)$ formæ pro numeris primis, *CCC* minoribus, calculavimus, et inde, vel etiam ex theoria residuorum, invenimus exponentem $\pm n$ minimum in schemate $\left(\begin{smallmatrix}+n\\ 1\ .\end{smallmatrix}\right)$ numerorum p hujusmodi:

$\begin{cases} p = 3,\ 7,\ 11;\ 13,\ 17,\ 19;\ 23,\ 29,\ 31;\ 37,\ 41,\ 43; \\ \pm n = +1, -3, -1; -3, -8, -9; -11, -14, +15; +3, +5, +21; \end{cases}$

$\begin{cases} p = 47,\ 53,\ 59;\ 61,\ 67,\ 71;\ 73,\ 79,\ 83;\ 89, \\ \pm n = -23, +13, -29; -31, +33, +35; -4, +13, +41; +44, \end{cases}$

$\begin{cases} p = 97,\ 101;\ 103,\ 107,\ 109;\ 113,\ 127,\ 131;\ 137,\ 139,\ 149; \\ \pm n = -48, -2; -17, +53, -54; -56, -63, -65; -4, -23, -74; \end{cases}$

$\begin{cases} p = 151,\ 157,\ 163;\ 167,\ 173,\ 179;\ 181,\ 191,\ 193;\ 197, \\ \pm n = +75, -39, +81; -83, +43, -89; -90, +95, -96; -49, \end{cases}$

---

*) Numeros in unciis formæ ( ) inclusos ex antecedentibus compositos vides; numerorum vero hujusmodi unciis [ ] circumdatorum factores non perquisivimus; horum vero plerosque scrutatus est Arithm. Docens Mag. M. Agardh, primosque invenit, præterquam 35 932 447, cujus factores sunt 4093 et 8779. Numeri vero 2906161 factores ex Tabula D^{ni} Burchkard eligantur.

$$\begin{cases} p = & 199, & 211; & 223, & 227; & 229, & 233, & 239; & 241, & 251, \\ \pm n = & +99, & -15; & -111, & +113; & -114, & -116, & +7; & -15, & -125, \end{cases}$$

$$\begin{cases} p = & 257; & 263, & 269, & 271; & 277, & 281, & 283; & 293, & 307. \\ \pm n = & -128; & -131, & -134, & +5; & +69, & -14, & +141; & +73, & +153. \end{cases}$$

Numerus vero n vel $2n$, prout signum $+$ vel $-$ adest, periodum decimalem indicat.

Universim vero, exsistente $p = 2n+1$ numero primo, schema $\binom{+2n}{1.}$ pro p valet; quoniam ex theoremate Fermatico $10^{2n} \underset{p}{\backsim} 1$, seu $10^{2n}-1 \underset{p}{\backsim} 0$. Quid quod $\binom{+n}{1.}$ valet, si 10 residuum est quadraticum ipsius p; sin minus, $\binom{-n}{1.}$ valet; hoc est $\binom{+n}{1.}$, si $\left(\frac{10}{p}\right) = +1$, et $\binom{-n}{1.}$, si $\left(\frac{10}{p}\right) = -1$. Tum enim est $10^n \backsim \left(\frac{10}{p}\right) \backsim \pm 1$, ideoque $10^n \mp 1 \underset{p}{\backsim} 0$. Ex lege vero reciprocitatis cel. LeGendre concluditur, $\left(\frac{10}{p}\right) = +1$ fore, exsistente numero primo $p \underset{40}{\backsim} \pm (1, 3, 9, 13)$, seu p, per 40 diviso, residua ± 1, ± 3, ± 9, ± 13 subministrante; e contra vero $\left(\frac{10}{p}\right) = -1$, si $p \underset{40}{\backsim} \pm (7, 11, 17, 19)$. Est enim $\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right) . \left(\frac{5}{p}\right)$, et $\left(\frac{2}{p}\right) = +1$, cum $p \underset{8}{\backsim} \pm 1$, seu $p \underset{40}{\backsim} \pm 1, \pm 7, \pm 9, \pm 17$; atque $\left(\frac{2}{p}\right) = -1$, cum $p \underset{8}{\backsim} \pm 3$, seu $p \underset{40}{\backsim} \pm 3, \pm 11, \pm 13, \pm 19$ atque $\left(\frac{5}{p}\right) = -1$, cum $p \underset{10}{\backsim} \pm 3$, seu $p \underset{40}{\backsim} \pm 3$, ± 7, ± 13, ± 17, $\left(\frac{5}{p}\right)$ vero $= +1$, cum $p \underset{10}{\backsim} \pm 1$, seu $p \underset{40}{\backsim} \pm 1, \pm 9,$

$\pm 11, \pm 19$. Erit igitur $\left(\frac{2}{p}\right).\left(\frac{5}{p}\right) = +1$, cum $p \underset{40}{\backsim} \pm 1, \pm 3, \pm 9, \pm 13$, atque $\left(\frac{2}{p}\right).\left(\frac{5}{p}\right) = -1$, cum $p \underset{40}{\backsim} \pm 7, \pm 11, \pm 17, \pm 19$. Inde vero concluditur, *schema* $\begin{pmatrix} +n \\ 1 . \end{pmatrix}$ *de numero primo* $2n+1 \underset{40}{\backsim} \pm(1,3,9,13)$, *seu qui a multiplo ipsius* 40 *cum differentia* 1, 3, 9, *vel* 13 *distat, semper valiturum; e contra vero* $\begin{pmatrix} -n \\ 1 . \end{pmatrix}$ *ad* $2n+1$ *formæ* $\underset{40}{\backsim} \pm (7, 11, 17, 19)$ *seu ad numerum primum a* $40 . m$ *cum* 7, 11, 17 *vel* 19 *distantem, attinere.*

Sin vero præterea fuerit $n = 2r$, vel $n = 3r$, vel $= 4r$ &c.,.. hujusmodi schematis exponens aliquando ex theoria residuorum potestatum altiorum adhuc non satis exculta inveniri potest aliquoties minor. (Pro cubicis cel. Jacobi, pro biquadraticis Cel. Gaussii valent regulæ, quas consulas).

Sic ex. gr. (ex tabula modo exhibita) videmus, numeris plerisque primis (p) esse indicem schematis $\begin{pmatrix} \pm m \\ 1 . \end{pmatrix}$ ejusmodi, ut $m = \frac{p-1}{2}$ sit, (nempe cum $p = 3, 7, 17, 19\ 23, 29, 31$ &c..), sicuti ex theoria residuorum quadraticorum elicuimus; in nonnullis vero m jam multo minor est; ut $m = \frac{p-1}{4}$, cum $p = 13, 53, 157, 173, 197, 277, 293$ &c., atque $m = \frac{p-1}{6}$, cum $p = 79, 103, 139$; — alias vero est $\frac{m}{p-1} = \frac{1}{8}, \frac{1}{10}, \frac{1}{12}, \frac{1}{14}, \frac{1}{16}, \frac{1}{18}, \frac{1}{20}, \cdot \cdot \frac{1}{34}, \cdot\cdot, \frac{1}{50}, \frac{1}{54}$ &c. cum $p = 41, 11, 37, 211, 241, 73, 281, \overbrace{137, 239}, 101, 271$: id quod ex theoria residuorum potestatum altiorum explicandum est.

Via modo explicata pauci tamen numerorum simplicium caracteres inveniuntur. Olim tamen, eadem progredientes, majus emolumentum exspectabamus, scribendo numerum quemvis datum (et quidem modo simplissimo, de quo olim agemus), signis dyadicis, triadicis &c...—

Ex dyadicis hæc tantum apponimus. Perquisimus scilicet factores numerorum formæ $2^n \pm 1$, quos heic vides:

$n =$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$2^n - 1 =$	1,	3,	7,	3.5,	31,	$3^2.7$,	127,	3.5.17,	7.73,	3.11.31,
$2^n + 1 =$	3,	5,	3^2,	17,	3.11,	5.13,	3.43,	257,	$3^3.19$,	$5^2.41$,

$n =$	11,	12,	13,	14,	15,	16,
$2^n - 1 =$	23.89,	$3^2.5.7.13$,	8191,	3.43.127,	7.31.151,	3.5.17.257,
$2^n + 1 =$	3.683,	17.241,	3.2731,	5.29.113,	9.11.331,	65537,

$n =$	17,	18,	19,	20,	21,
$2^n - 1 =$	131071,	$3^2.7.19.73$,	524287,	$3.5^2.11.31.41$,	$7^2.127.337$,
$2^n + 1 =$	3.43691,	5.37.109,	3.174763,	17.61681,	$3^2.43.5419$,

$n =$	22,	23,	24,	25,
$2^n - 1 =$	3.23.89.683,	47.178481,	$3^2.5.7.13.17.241$,	31.601.1801,
$2^n + 1 =$	5.397.2113,	3.2796203,	97.257.673,	3.11.251.4051.

$n =$	26,	27,	28,	29,
$2^n - 1 =$	3.2731.8191,	7.73.262657,	$(2^{14} \pm 1)$,	233.[2 304167],
$2^n + 1 =$	5.53.157.1613,	$3^3.19.261633$,	17.15790321,	3.59.[3 033169],

---

*) Hic numerus $(2^{31}-1)$ primus hucusque perquisitorum maximus videtur. Præterea observare licet, numeros formæ $\frac{1}{3}(2^n+1)$ tum plerumque primos esse, cum n primus sit; dantur tamen casus excipiendi, pauci forsan, ut cum $n=29$.

$$\begin{cases} n = & 30, & 31, & 32, \\ 2^n - 1 = & (2^{15} \pm 1), & 2147\,483647,^{*)} & (2^{16} \pm 1), \\ 2^n + 1 = & 5^2.13.41.61.1321, & 3.715\,827883, & 641.6\,700417. \end{cases}$$

Hinc et aliunde colligimus, minimum exponentem (n) schematis $(1^{n}_{.})$, quod numero dyadice scripto et secundum factorem primum (p) perquirendo præfigatur, fore sequentem:

$$\begin{cases} \text{cum } p = & 3, & 5, & 7, & 11, & 13, & 17, & 19, & 23, & 29, & 31, & 37, \\ \text{erit } n = & -1, & -2, & +3, & -5, & -6, & -4, & -9, & +11, & -14, & +5, & -18, \end{cases}$$

$$\begin{cases} p = & 41, & 43, & 47, & 53, & 59, & 61, & 67, & 71, & 73, & 79, \\ n = & -10, & -7, & +23, & -26, & -29, & -30, & -33, & +35, & +9, & +39, \end{cases}$$

$$\begin{cases} p = & 83, & 89, & 97, & 101, & 103, & 107, & 109, & 113, & 127, & 151, \\ n = & -41, & +11, & -24, & -50, & -51, & -53, & -18, & -14, & +7, & +15, \end{cases}$$

$$\begin{cases} p = & 233, & 241, & 251, & 257, & 331, & 337, & 397, & 601, & 673, & 683, & 1801, \\ n = & +29, & -12, & -25, & -8, & -15, & +21, & -22, & +25, & -24, & -11, & +25, \end{cases}$$

$$\begin{cases} p = & 2113, & 2731, & 4051, & 5419, & 8191, & 43691, & 61681, & \&c. \\ n = & -22, & -13, & -25, & -21, & +13, & -17, & -20, & \&c. \end{cases}$$

Sic ex. gr. dato numero (N) cujus signum dyadicum est 110 11011 00100 00101, seu hoc: (224389 =)
$N = 2^{17} + 2^{16} + 2^{14} + 2^{13} + 2^{11} + 2^{10} + 2^7 + 2^2 + 1$, et divisore $p = 31$, erit schema $\left(\begin{smallmatrix}+\nu\\ 1\,.\end{smallmatrix}\right)$, et $\left(\begin{smallmatrix}+\nu\\ 1\,.\end{smallmatrix}\right) N = 110 + 11011 + 100 + 00101 = 101010$, et iterum $\left(\begin{smallmatrix}+\nu\\ 1\,.\end{smallmatrix}\right).101010 = 1 + 01010 = 1011$ seu $= 2^3 + 2^1 + 1$, quod quidem est $= 11$ in signis vulgaribus decadicis, attamen incongruum ipsi $p (= 31)$, (utut multo minus), cujus signum dyadicum est 11111. Est igitur N per p non divisibilis, sed residuum $= 2^3 + 2 + 1$ ($= 11$) relinquit, (seu $N \underset{31}{\backsim} 11$).

Hac tamen via perpauci numeri primi caracteribus simplicibus præditi inveniuntur; aliam igitur ingrediendum est.

Perquirendi igitur sunt dati divisoris numeri auxiliares, in schematibus $\left(\alpha \overset{+\nu}{-} .\right)$, $\left(. \overset{\nu+}{-} \beta\right)$, $\left(\alpha \overset{+\nu}{-} . \beta\right)$ occurrentes, iique quamminimi.

I) Primum igitur numeri $\pm\alpha$ et ν in schemate $\left(\alpha \overset{+\nu}{-} .\right)$, ad divisorem datum (p) pertinentes, inveniuntur simplicissime et quidem eo modo, quo vulgaris fractio $\left(\frac{1}{p}\right)$ in decimalem convertitur.

Dividimus nempe more solito 10^n per (p), attamen ita, ut residuum vel positivum vel negativum sit et semper $<\frac{1}{2}p$; deinde eliguntur residua minima pro α, et exponentes n, his correspondentes, pro ν accipiuntur.

Sit. ex. gr. 1) $p=7$; erit $\frac{1}{7}=0,143\ldots$ 7|1000|143

30

20

−1

et residua 3, 2, −1 ad exponentes 1, 2, 3 pertinebunt, quare schemata primi generis, ad divisorem 7 pertinentia, erunt $\left(3 \overset{+I}{.}\right)$, $\left[2 \overset{+II}{.}\right]$, $\left[-1 \overset{+III}{.}\right]$ seu $\left[1 \overset{-III}{.}\right]$.

Ex. 2) Sit deinde $p=109$, erit

$$10^n \underset{p}{\backsim} 1,\ 10,\ 100\ (\text{seu} -9),\ 19,\ 81\ (\text{seu} -23),\ \&c.$$

prout nempe exponens $n=0,\ 1,\ 2,\ 3,\ 4$ &c.. fuerit.

Obs. Cum divisio vulgari modo aliquot passus instituta fuerit, reliqua, si simplex aliqua residuorum jam inventorum ratio observatur, brevius perficitur. In ex. sc. allato residuum tertium